UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/506,158	02/17/2000	Pierre-Yvan Liardet	98RO21054169	6798

27975 7590 07/16/2004

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
ADAMS, JONATHAN R	

ART UNIT	PAPER NUMBER
2134	9

DATE MAILED: 07/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/506,158	LIARDET ET AL.	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: amendment filed 4/15/2004 to the application filed 2/17/2000.

Independent claims have been amended: Claims 11, 17, 25, and 30.

Dependant claims 13,18, 19, 21, 22, 27, 28, 32, and 33 have been amended.

Claims 26 and 31 have been cancelled.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 11, 12, 14-16, 17, 18, and 20-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Smith, Sr. et al. (US Patent no. 6,144,744, hereafter referred to as '744) in view of applicant admitted prior art.

4. As to claims 11:

Applicant admitted prior art sited in Fig. 3 teaches a system/apparatus/circuit comprising:

- Memory module for storing... (Fig 3, Item 30, Applicant Admitted)
- Input/Output registers (Fig 3, Item 32, Applicant Admitted)
- Two-Way link (Fig 3, Item 31, Applicant Admitted)
- Input register (Fig 3, Item 36, Applicant Admitted)

- Key register (Fig 3, Item 38, Applicant Admitted)
- Multiplexer (Fig 3, Item 34, Applicant Admitted)
- Processing module (Fig 3, Item 42, Applicant Admitted)
- Control module (Fig 3, Item 40, Applicant Admitted)
- Output register (Fig 3, Item 44, Applicant Admitted)

5. Applicant admitted prior art does not teach the use of scrambling bits to secure the value of the digital key. '744 teaches a method for the secure transfer of data between secure component modules using scrambling bits to ensure the secure transfer of data and a digital key during the transmission to\from the connected processor (Col 5, Line 32, '744):

- Scrambling register... / the transport key is stored in the BTK register...(Col 16, Line 16 et seq., '744)
- Receiving digital key data from memory module comprising digital key and scrambling bits intermixed with digital key / Determining digital key based on digital key data and scrambling bits / Authority establishes a transport key, at the end of this step transport key is stored in BTK register... Encrypts key part under transport key... loads/decrypts obtained key part (Col 16, Lines 13-36, '744)

6. It would have been obvious to a person of ordinary skill in the art at the time of invention to combine the invention submitted as prior art by the applicant with the invention described in '744. One of ordinary skill in the art would have been motivated to augment applicant admitted prior art because "it is desirable to have a way to transfer the master key from one cryptographic processor to another" (Col. 1, Line 58 et seq.,

'744). '744 suggests that the crypto module may be physically integrated into a central processor complex of a general purpose digital computer (Col. 5, Line 58 et seq., '744).

7. As to claim 12:

Scrambling bits are foreign to / Extracted key under the transport key ...(Col 2, Line 62 et seq., '744)

As to claim 14:

8. '744 as modified above teaches the use of an accessory input register and a scrambling register to aid in the security of a cryptographic coprocessor. Not specifically taught is to implement the accessory input register as being the same size as the scrambling register. The examiner takes official notice to implement the accessory input register as being the same size as the scrambling register. It would have been obvious to a person of ordinary skill in the art at the time of invention to implement the accessory input register as being the same size as the scrambling register. One of ordinary skill in the art would have been motivated to implement the accessory input register as being the same size as the scrambling register because the size of the register under the circumstances is considered to be arbitrary, as "there is no major drawback if the accessory input register has a size different from that of the scrambling register" as sited in the specification (Page 13, Line 7 et seq.).

9. As to claim 15:

Scrambling bits are generated randomly / Pseudo Random number generator (Fig. 1, Item 160, '744)

10. As to claim 16:

Scrambling bits are sent in groups of eight bits / 16-byte (128-bit) crypto identifier (Col 6, Line 9 et seq., '744)

11. As to claims 17, 18, and 20-34:

Claims 17, 18, and 20-34 correspond to claims 11, 12, and 14-16

12. Claims 13 and 19 rejected under 35 U.S.C. 103(a) as being unpatentable over '744 in view of applicant admitted prior art in further view of "80x86 evolution".

As to claims 13 and 19:

13. '744 as modified above teaches a system for the secure transfer of data between secure component modules using scrambling bits to ensure the secure transfer of data connected to a central processing unit (Col 5, Line 32, '744). '744 as modified above does not teach an accessory input register between processing module and scrambling register. 80x86 evolution teaches a working/input register connected between the processing ALU and input from outside sources (Page 7, Fig 1, 80x86). It would have been obvious to a person of ordinary skill in the art at the time of invention to use an 80x86 style processor in conjunction with '744 as modified above. One of ordinary skill in the art would have been motivated to use an 80x86 style processor in conjunction

with '744 as modified above because the 80x86 style processor is one of the most commonly used and readily available processors on the market.

14. As to claims 17-34:

Claims 17-34 correspond to claims 11-16.

.Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

16. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (703)

305-8894. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306 Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100